THE DIR CYBERSECURITY INSIGHT

Happy New Year

New Year's Resolution: Maintain Your Security Fitness

As we pack away all our holiday ornaments and decorations and list our New Year's resolutions (save more money, get to the gym!), we start to look at what's to come in the year ahead both in our personal and professional lives. How can we improve our security fitness in 2017 with current resources? How will the upcoming legislative session affect our security programs?

Here are a few things to consider when building your approach to maintainable security fitness:

Awareness. Ensuring that management understands the need for a comprehensive security program can help the ISO focus on the best direction the program should take for the organization.

Strategic-Level Vision. Security programs need a direction, a clear path based on the organizational mission. This direction includes documented goals along with a governance process to define how that vision will be implemented.

People, Processes, and Technology. These three pillars of a security program, when working in tandem, are building blocks of a strong security program. People are your resources. They implement your vision. Processes provide structure, consistency, and a formally documented approach to how you manage your security program. And the technology, when implemented properly, can move your security program from a reactive state to a risk-based, proactive state.

Communication. Communicating meaningful metrics to your executive leadership can prove the viability of your program and help maintain strong leadership support. In addition, forming strong working relationships with peers in other departments within IT and other business units can demonstrate the security team can add value to projects that support the business mission while better protecting the data.

CONTENTS

EVENTS

Save the Date

- **Data Privacy Day**: January 28
- **TASSCC TEC 2017**: Friday, March 31
- **Information Security Forum**: April 11-12, 2017, Palmer Events Center,

DIR

Dept. of Information Resources

InfoSec Academy Update

The next (and most likely last) opportunity to take the Texas Security Policy & Assurance course in a classroom setting is on Jan. 20, 2017. You must complete this course prior to starting any of the certification prep courses offered through the academy (Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified in Risk and Information Systems Control (CRISC), CompTIA Security+ and Certified Ethical Hacker (CEH). Click here to enroll in the instructor led Texas Security Policy & Assurance class. To learn about the Texas InfoSec Academy and course offerings, visit the Texas InfoSec Academy.

Gartner Webinars

Below are three **new** and relevant on-demand security webinars from which to choose! To watch the webinar, please click on the underlined session title below, and you will be taken directly to it. You will also be able to download the presentation from the main landing page, as well. If you have any difficulties accessing the webinars, please send an email to Joe Martin (joe.martin@gartner.com). If you are interested in speaking with a Gartner analyst to interactively discuss the material presented in the on-demand webinar, please contact Steve Reda (steve.reda@gartner.com) to coordinate.

Building Successful Business Metrics for Technology Risk

Security and risk management leaders are always trying to improve the quality of their metrics to inform better decision making in their organizations. "Business alignment" is spoken about frequently, but execution is challenging. Key risk indicators (KRIs) should have defensible causal relationships to business impacts and present leading indicators to decision makers. In this webinar, we discuss a Gartner methodology to integrate risk and corporate performance that helps achieve these goals.

Hosted by: Jeffrey Wheatman

Safeguard Critical Systems with Privileged Account Management

The need to govern and secure privileged access has grown dramatically as today's digital businesses push resources to the cloud and outsource critical business functions to third parties. In this video, we discuss how organizations can implement a risk-based approach to prioritize and architect a privileged account management (PAM) implementation.

Hosted by: Lori Robinson

How to Fortify Your Endpoint Security by Making Application Control Work

Various solutions protect against sophisticated and unknown malware by controlling applications on the endpoint. Examples are application whitelisting, privilege management and application isolation.

Hosted by: Mario de Boer

SPECTRIM

SPECTRIM changes coming soon! In March, we will be upgrading to Archer 6.1 which is designed to offer an enhanced user experience with a simpler but more powerful user interface and advanced workflow capabilities. We will not be changing any functionality with this upgrade. We will upgrade our development and test environments on Feb. 27, and will be providing screen shots and instructions about the changes during the following three-week period. Production will be upgraded on March 20, 2017. Please plan for SPECTRIM to be unavailable on this day

DIR
Dept. of Information Resources

Data Privacy Day

"After a while, you learn that privacy is something you can sell, but you can't buy it back."—Bob Dylan

January 28 - an international day dedicated to creating awareness about privacy and data protection. In the most basic of terms your identity belongs to you. Most people freely enjoy the privilege of personal privacy. But what if this is compromised by a bad actor? Your personal information could be exploited, sold, or even used against you. Knowledge is power and January 28 is a day to empower yourself and your team. Taking precautionary steps and being able to identify risks and threats can protect you and your family's personal information and privacy. You can share your knowledge, protect yourself and get involved. Here are a few tips from Stay Safe Online to protect your privacy and identity:

Share with Care

- What you post can last a lifetime: Before posting online think about how it might be perceived now and in the future and who might see it.
- Own your online presence: Set the privacy and security settings on web services and devices to your comfort level for information sharing. It's ok to limit how and with whom you share information.
- Be aware of what's being shared: Be aware that when you share a post, picture or video online, you may also be revealing information about others. Be thoughtful when and how you share information about others.
- Post only about others as you have them post about you: The golden rule applies online as well.

Personal Information Is Like Money. Value It. Protect It.

- Think before you act: Be wary of communications that implore you to act immediately, offer something that sounds too good to be true or ask for personal information.
- Get two steps ahead: Switch on two-step verification or multi-factor authentication wherever offered to prevent unauthorized access.

Support Data Privacy Day:

- Share on social media using the hashtag #DataPrivacyDay
- Visit and share StaySafeOnline for facts and tips about protection.

Security with Raspberry Pi

What started as a novel idea to encourage programming and promote computer science in schools, Raspberry Pi PCs (RPs) have become a springboard for creativity and innovation to our social media generation. These credit card-sized, mini PCs have been used to demonstrate some of the most inventive and astonishing DIY projects of the 21st century. They've been used to power robotics, UAVs, create home NAS servers, media players, nostalgic video game emulators, and even cat food feeders. Their applications are only limited by the imagination.

So, when I found my own Pi under the tree this past Christmas I was very excited. It also fed my curiosity regarding their use in security applications. After doing some research online, I was amazed to find how a simple Raspberry Pi (and a little programming knowledge and corresponding hardware) can provide an abundance of personal security features. Here are just a few ideas that others have shared:

Treasure Box. These are essentially safes, but with programmable facial recognition. It's like having a bank's safety deposit box in the convenience of your own home.

Home Firewalls and IDS. Firewalls help to protect networks from malicious attacks, while IDSs are used to detect when an intrusion into your network has occurred. With a copy of Linux and some disk management software, Raspberry Pis can be used to protect precious personally identifiable information in your home network.

Home Security System. Okay, like many things on this list, this DIY project takes more than just a Raspberry Pi. However, it doesn't take much to setup and you can skip monthly third-party monitoring service fees because you can monitor it from the convenience of a smart device.

Surveillance Camera. Buying a *fake* surveillance camera may work for deterrence, but install a programmed Raspberry Pi inside and suddenly you have a working, facial recognition and even motion-detection surveillance camera, at a reasonable price.

Smart Doorbell. If you haven't heard of them [Thank you, makeuseof.com!], smart doorbells alert occupants from anywhere inside the home (or outside the home, provided you have a smart device) when someone approaches. They usually have built-in Wi-Fi capabilities, motion-sensing, video recording and even personalized voice messaging. Crazy, right?! However, they can be rather expensive. A Raspberry Pi PC can make a DIY version affordable for those on a budget.

Wardriving. This isn't so much of a security feature that Raspberry Pi PCs provide, then it is a security risk. For those unfamiliar with the term, *wardriving* essentially means actively searching for open Wi-Fi networks by a person who is mobile – usually in a car or on a bicycle. With Raspberry Pi's convenient size and low power consumption, it makes mobility easier for wardriving than hauling around bulking laptops.

If you're interested in learning more, I encourage you to check out www.raspberrypi.org for a list of DIY projects and community forums.

OCISO Corner

Angela Gower
Information Security Analyst
Department of Information Resources

What is your responsibility in DIR and with the State?

I'm an Information Security Analyst and my role is to support the statewide information sharing of cybersecurity incident response.

When and where did you start your career?

While working part-time at an organization during my freshman year of college, the executive director asked for volunteers interested in helping to install a computer network (Novell 3.11!). I was the only person who volunteered. I enjoyed the project and once installed, they needed someone to maintain it. I had found something I enjoyed and wanted to do more of—I was hooked. The company hired me as the IT person and that began a nine-year experience of IT immersion into networks, database management, software and hardware installation along with user training.

Why security field?

After 20+ years of working in various IT roles ranging from help desk to network administration to database management, moving to an Information Security specialization allowed me to leverage my IT experience to help others protect their data.

What did you think you were going to be when you grew up?

A teacher.

What is the greatest lesson you have learned?

"Be able to laugh at yourself and make others laugh" and "Kindness—in all sizes— matters."

What do you want your legacy to be?

From a professional perspective, I would hope that any user I provided IT or information security assistance to, throughout my career, would remember that there are no stupid questions and wouldn't show any fear in asking those questions. Sometimes the questions a user hesitates to ask are critical to a successful outcome.

Do you have a favorite hobby or pastime?

I enjoy being outdoors.

What do you like best about working at DIR?

The people. They've been extremely friendly and helpful to me—before and after I joined the agency.

THE DIR CYBERSECURITY INSIGHT

DIR
Dept. of Information Resources